



February 17, 2012
Via ECFS Filing

Ms. Marlene H. Dortch, Secretary
Office of the Secretary
Federal Communications Commission
9300 East Hampton Drive
Capitol Heights, MD 20743

RE: X2Comm, Inc. d/b/a DC Communications
Annual CPNI Filing
EB Docket No. 06-36; 2011

Dear Ms. Dortch:

Attached for filing is the Calendar Year 2011 CPNI Compliance Certification and Statement of CPNI Procedures and Compliance as required by 47 C.F.R. Section 64.2009(e) submitted on behalf of X2Comm, Inc. d/b/a DC Communications.

Any questions you may have regarding this filing should be directed to my attention at (407) 740-3031 or via email at stthomas@tminc.com. Thank you for your assistance in this matter.

Sincerely,

/s/Sharon Thomas
Consultant to X2Comm

cc: Best Copy and Printing, Inc. - FCC@BCPIWEB.COM
Chief, Telecommunications Consumers Division, Enforcement Bureau, FCC
file: Tina Tecce - FCC - Other
tms: FCx1201

Enclosures
ST/im

EB Docket 06-36

Covering calendar year 2011

X2 Comm, Inc. d/b/a DC Communications

821794

Mark Pavol

Secretary/Treasurer

- [Handwritten signature]*

111

0 | 14 | 12

Attachments: Accompanying Statement explaining CPNI procedures

Attachment A
Statement of CPNI Procedures and Compliance

X2 Comm, Inc. d/b/a DC Communications

Statement of CPNI Procedures and Compliance

X2 Comm, Inc. d/b/a DC Communications ("X2 Comm" or "the Company") does not use or permit access to CPNI to market any telecommunications or non-telecommunications services. X2 Comm has trained its personnel not to use CPNI for marketing purposes. Should X2 Comm elect to use CPNI in future marketing efforts, it will follow the applicable rules set forth in 47 CFR Subpart U, including, if necessary, the institution of operational procedures to ensure that notification is provided and customer approval is obtained before CPNI is used or disclosed.

X2 Comm has put into place processes to safeguard its customers' CPNI from improper use or disclosure by employees; and to discover and protect against attempts by third parties to gain unauthorized access to customer CPNI. The Company maintains all CPNI in a secure server environment with limited access. The Company trains its employees regarding the requirements to safeguard CPNI against unauthorized disclosure and has a disciplinary process in place.

X2 Comm does not disclose CPNI to any agents, affiliates, joint venture partners or independent contractors, nor does it use CPNI to identify or track customers who call competing providers. The Company has a strict policy prohibiting the disclosure of CPNI to any third parties, unless required to do so by law (e.g., in response to a subpoena). X2 Comm maintains a record of all instances where CPNI was disclosed or provided to third parties, or where third parties were allowed access to CPNI as a result of a legally authorized request.

X2 Comm does not disclose CPNI over the telephone in response to a customer-initiated telephone inquiry, unless the customer can provide the call detail information that is the subject of the inquiry without the assistance of a customer service representative. If it elects to do so in the future, it will follow the applicable rules set forth in 47 CFR Subpart U, including the implementation of authentication procedures that do not require the use of readily available biographical information or account information and customer notification of account changes.

If a customer's account information is changed, the Company immediately notifies the customer of the change via e-mail to the e-mail address of record (before the change), without revealing the changed information.

The Company does not disclose CPNI on-line. If it elects to do so in the future, it will follow the applicable rules set forth in 47 CFR Subpart U, including the implementation of authentication procedures that do not require the use of readily available biographical information or account information and customer notification of account changes.

X2 Comm does not have any retail locations and therefore does not disclose CPNI in-store.

The Company has procedures in place to notify law enforcement in the event of a breach of customers' CPNI and to ensure that the affected customers are not notified of the breach before the time period set forth in the FCC's rules, or, if applicable, when so authorized by law enforcement. Specifically, as soon as practicable, and in no case later than seven business days upon learning of a breach, the company will notify the U.S. Secret Service and the FBI by

electronic means, as required by FCC regulations. The company will not notify customers or disclose a breach to the public until seven full business days have passed after notification to the U.S. Secret Service and the FBI, unless it believes there is an extraordinarily urgent need to notify customers before seven days in order to avoid immediate and irreparable harm. In that instance, it will only notify such customers *after* consultation with the relevant investigating agency and will cooperate with the agency's request to minimize any adverse effects of the customer notification. If the Company receives no response from law enforcement after the seventh full business day, it will promptly proceed to inform the customers whose CPNI was disclosed of the breach. The company will delay notification to customers or the public if requested to do so by the U.S. Secret Service or FBI. Notifications to law enforcement and customers are handled by a designated supervisor level employee responsible for managing the company's CPNI compliance.

The company has processes in place to ensure that it maintains electronic records of any breaches that are discovered and of notifications made to the USSS and the FBI, as well as to customers, for a period of at least two years. Information regarding any breaches and notifications will be maintained by a designated supervisor level employee responsible for managing the company's CPNI compliance.

X2 Comm has not taken any actions against data brokers in the last year.

X2 Comm did not receive any customer complaints about the unauthorized release of CPNI or the unauthorized disclosure of CPNI in calendar year 2011.

Company has not developed any information with respect to the processes pretexters are using to attempt to access CPNI. If the Company suspects that a pre-texter may be attempting to gain access to CPNI, it will immediately ask the requester to provide information that only the customer would be able to provide and would further investigate suspected pre-texting activity.